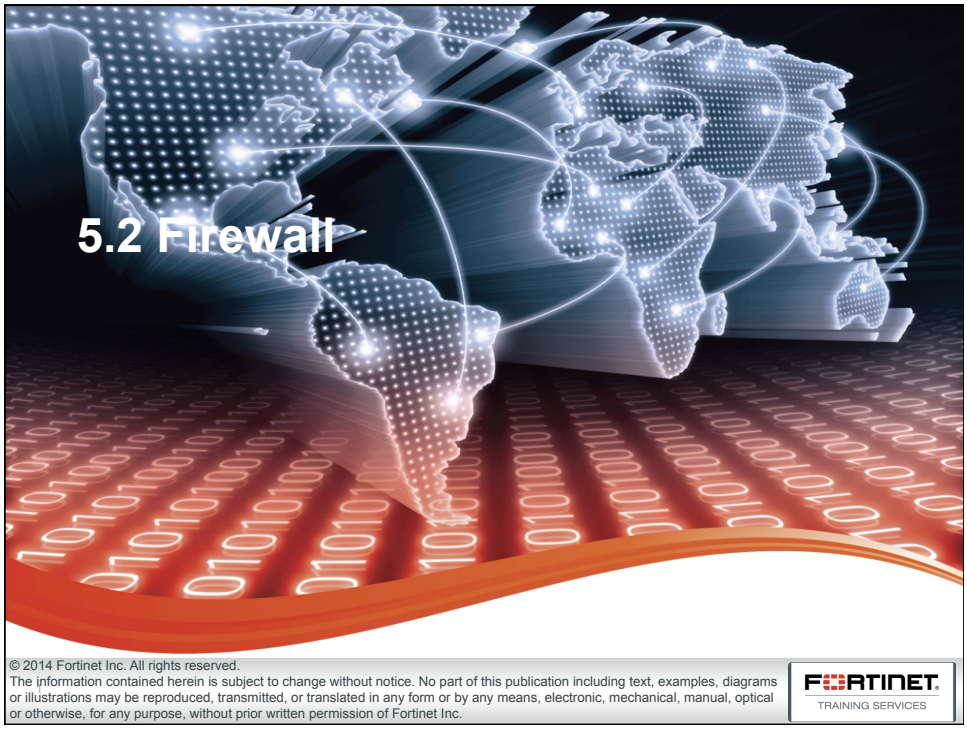


Logging & Reporting: New Features & Changes

- NAC Quarantine simplification
- Captive Portal
- HTTP header replacement for Virtual Servers
- IPv6
- TCP Reset when session automatically closed
- CoS Support

NAC Quarantine simplification

- Many quarantine options have been removed. They will be added back in Future firmware versions.
- DLP sensor: only option is quarantine-ip to quarantine all traffic from the IP address.
- Antivirus profile: only option is quar-src-ip to quarantine all traffic from the source IP.
- IPS sensor: only option is block attacker's IP.
- IPv4 & IPv6 DoS-policies: only option is attacker to block attacker's IP.

3

Captive Portal

- In 5.0, Captive portal was a mechanism for capturing authentication through the wireless
- In 5.2, Captive portal is used for capturing user authentication on an interface (wireless or otherwise)

4

HTTP header replacement for Virtual Servers

- By default, if http-ip-header is enabled in a virtual-server configuration then as HTTP(S) traffic flows through a virtual server FortiOS either adds an *X-Forward-For* header with the client's original IP address or updates any existing *X-Forwarded-For* header with the client's IP address. Some servers want the client's original IP address, but do not want to use *X-Forwarded-For* and instead want a configurable name to be used. The new attribute http-ip-header-name allows this name to be defined.
  - » If defined, then any existing X-Forwarded-For header is removed.

5

HTTP header replacement for Virtual Servers: CLI Config

```
config firewall vip
       edit (vip name)
       set type server-load-balance
       set server-type https
       Set http-multiplex enable
       set http-ip-header enable
       set http-ip-header-name <name of header to add>
end
```

- `server-type` of http and `http-mutiplex enable` are required settings to be use this functionality.

6

IPv6: TCP Clamping

- 5.0.x (and previous) and TCP Clamping for IPv4 (CLI Only, per policy)

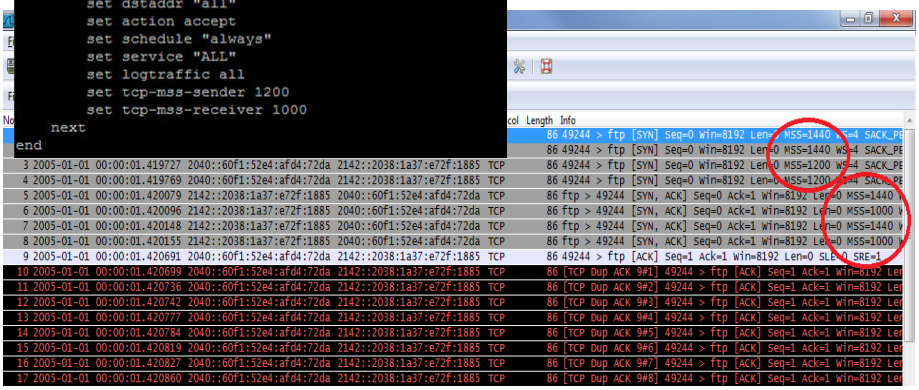
```
config firewall policy
      edit (policy id)
               set tcp-mss-sender [MSS value to set on egress traffic]
               set tcp-mss-receiver [MSS value to set on ingress traffic]
      end
```

- 5.2 adds support in IPv6 policies
  - » IPv6
  - » NAT66
  - » NAT46/NAT64

7

IPv6: TCP Clamping (Wireshark)

```
FortiGate-VM64 (1) # sh
config firewall policy6
    edit 1
        set uuid 87b4d704-9b1c-51e3-3772-ef3239e6a244
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set tcp-mss-sender 1200
        set tcp-mss-receiver 1000
    next
end
```



8

IPv6: Reverse Path Forward (RFP)

- RFP support added for IPv6

```
id=13 trace_id=9 func=resolve_ip6_tuple_fast line=2737 msg="vd-root received a packet(proto=58, 2040::47:22272->2060::54:128)

from port1."
id=13 trace_id=9 func=resolve_ip6_tuple_fast line=2737 msg="vd-root received a packet(proto=58, 2040::47:22272->2060::54:128) from port1."
id=13 trace_id=9 func=resolve_ip6_tuple line=2828 msg="allocate a new session-0001d805"
id=13 trace_id=9 func=vf_ip6_route_input line=458 msg="reverse path check failed, drop"
id=13 trace_id=9 func=ip6_session_handle_no_dst line=2853 msg="trace"
```


TCP Reset when session automatically closed

- Some protocols remain open but send no data unless there is a change
  - » Example: RDP
  - » Connection is TCP based but no traffic is sent unless there is something from the client or server to update
  - » Default Session timeout is 3600 seconds (1 hour)
  - » After 1 hour of no activity the FortiGate will close down the session. This could result in the loss of connectivity and no error message on the client or server.

TCP Reset when session automatically closed: policy

- Enabled in CLI per firewall policy

```
config firewall policy
     edit (policy_id)
        set timeout-send-rst enable
     end
```

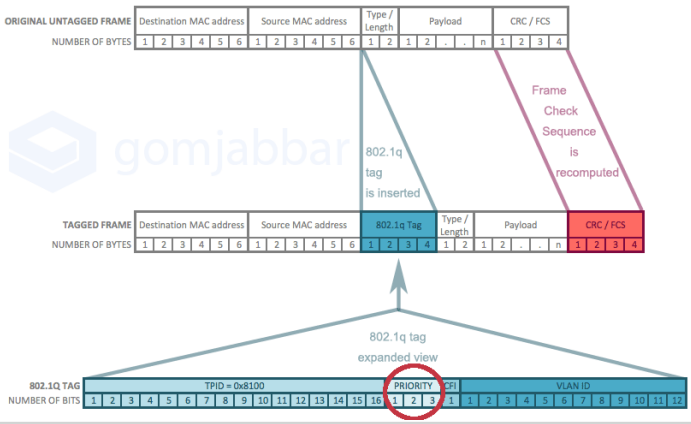

CoS: What is it?

- Class of Services (COS)
  - » Defined by 802.1p IEEE standard

Priority	Acronym	Traffic Types
0 (lowest)	BK	Background
1	BE	Best Effort
2	EE	Excellent Effort
3	CA	Critical Applications
4	VI	Video (< 100 ms latency and jitter)
5	VO	Voice (< 10 ms latency and jitter)
6	IC	Internetwork Control
7 (highest)	NC	Network Control

CoS: What does it look like in the packet?

- a 3-bit field within an Ethernet Frame of TCP/IP Layer 2.
  - » Part of the 802.1q tag extension for Vlans



CoS: Upgrading

- Previous firmware did not preserve the CoS information in the packets. It was removed.
- 5.2 will now (by default) preserve this information on packets as they passes through
  - » May result in different network behavior since previously information may have been stripped off.

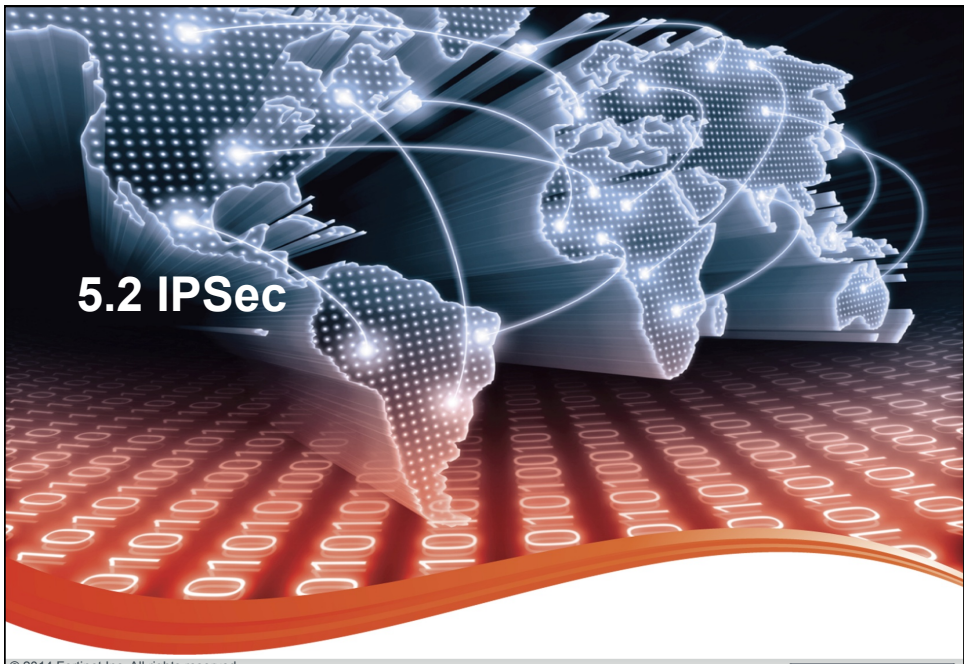
CoS: Preserve or set?

- Value for CoS in the packets can be preserved or modified on a per IPv4 or IPv6 policy basis
  - » <value> may be : 0,1,2,3,4,5,6,7,255 (255 means passthrough)

```
config firewall [policy|policy6]
       edit (id_number)
              set vlan-cos-fwd (value)
              set vlan-cos-rev (value)
       end
```

15

FORTINET



FORTINET TRAINING SERVICES

VPN: New Features & Changes

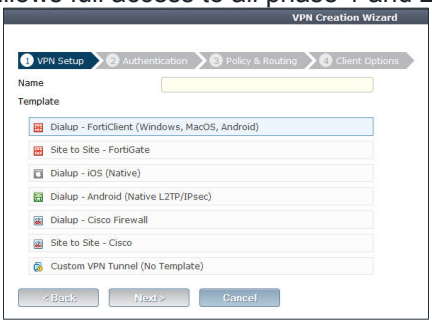
- IPSec Wizard
- Menu Squish
- Automatically route addition
- Multiple interface support
- Authentication against groups
- IPv6 for quickmodes
- IKEv2 cookie notification
- DH Negotiation & Encryption

IPSec: Wizard (GUI only)

- Creation and Editing of IPSec VPNs is done via the VPN Wizard
- Only Interface based VPNs can be created through the Wizard
  - » Initial Tunnel up policy automatically created
  - » Route(s) automatically added (only Site-to-site)
  - » VPNs created from the CLI do not invoke the GUI Wizard
- Editing Interface VPNs automatically updates routes and policies
- Unable to delete VPN created incorrectly
  - » Policy & Route(s) must be deleted first (object dependency)

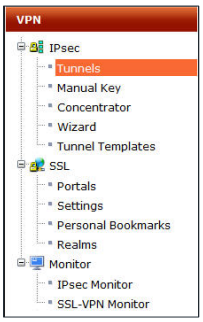
IPSec: Wizard Options

- Default templates stored for multiple devices
  - » Automatically set various phase1/2 to device defaults for 3rd party vendors
  - » FortiClient, FortiGate, Cisco, iOS, Andriod
  - » 'Custom' allows full access to all phase 1 and 2 settings



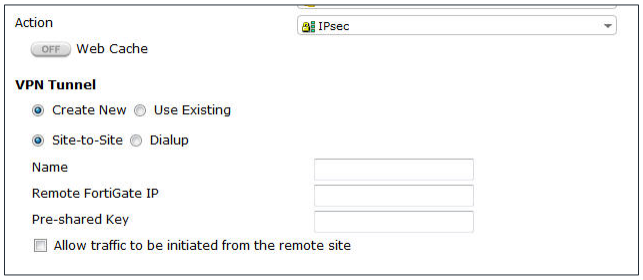
Menu Squish

- 5.0 saw the start of a large push to "Make the FortiGate easier to configure"
- Rather then 2 separate menu options IPSec and SSLVPN are moved into a single menu
  - » Not the only section where this has happened



IPSec: Policy VPNs in the GUI

- Creating policy VPNs in GUI requires enabling the option in 'features'
  - » Create policy based VPNs via firewall policy using action 'IPSec' (or CLI)



21

IPSec: Automatic route addition (CLI only)

- Intended for use with BGP over IPSec
- Previously the option was only available in phase 1 when mode-cfg was enabled
  - » Can be used in phase 1 /phase 2 on any dynamic VPN

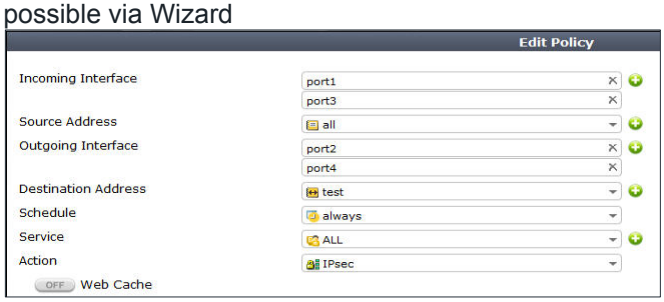
```
config vpn ipsec [phase1|phase1-interface|phase2|phase2-interface]
      edit (vpn name)
            set type dynamic
            set add-route enabled              (phase 1 and phase 2)
            set distance [0-255]               (phase 1 only)
            set priority [0 - 4294967295]      (phase 1 only)
      end
```

- Automatically adds route to routing table when tunnel is up

22

IPSec: Multiple interface support

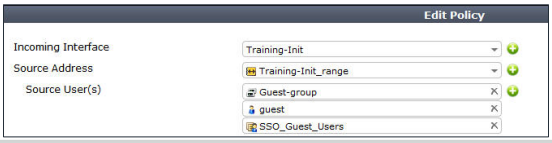
- IKE/IPSec Policys can now be set to include multiple interfaces
  - » Eliminates need to configure duplicate VPN on a separate interface for redundancy
  - » Works for both Policy and interface based IPSec tunnels
  - » Not possible via Wizard



23

Authentication against groups

- Rather then specify the authentication groups in the Phase 1, they can be specified within the VPN firewall policy itself.
- Available for “Dialup” VPNs
  - » XAuth can be changed by editing the VPN after it’s been created



24

IKEv2 cookie notification

When the FortiGate unit detects that the number of half-open IKEv2 SAs is above the threshold value, to preserve CPU and memory resources, the IPSec VPN dialup server requires all future SA_INIT requests to include a valid cookie notification payload that the server sends back.

RFC 5996, Section 2.6

- Exact value is hard coded (not configurable) and based on the model.
  - » Small models 1000
  - » Larger models 10,000+

25

IPv6 for quickmodes

- Address objects in phase 2 quickmode selectors now support IPv6 addresses

26

DH Negotiation & Encryption

- Default DH group adjusted to include 14 and 5
- Support added for up to 3 DH groups in both Phase 1 and Phase 2
- ECDSA-256, ECDSA-384, ECDSA-512 auth methods added
  - » RFC 4754

VPN: New Features & Changes

- IPSec Wizard
- Menu Squish
- Automatically route addition
- Multiple interface support
- Authentication against groups
- IPv6 for quickmodes
- IKEv2 cookie notification
- DH Negotiation & Encryption

29

Client Reputation: New Features & Changes

- Summary of Changes over 5.0.x
- Renamed and moved

30

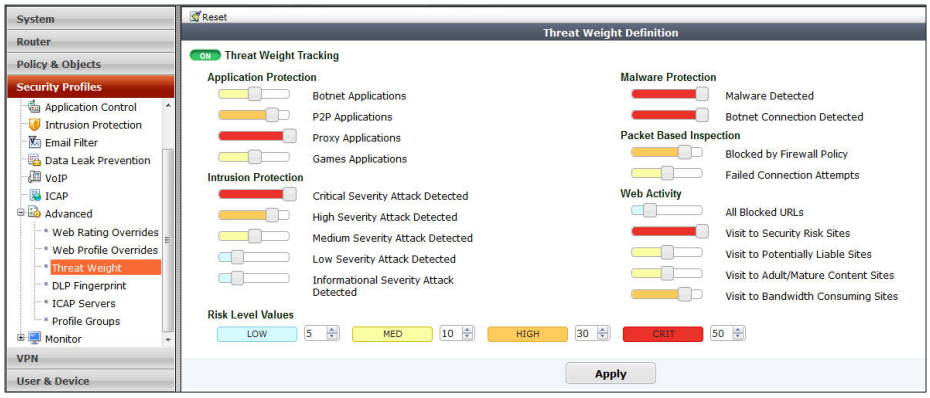
Client reputation: Summary of Changes over 5.0.x

- 5.0.0 any device can enable
  - » Monitoring is done via Client Rep monitor (available on 60+)
  - » Requires SQL logging enabled
- Patch 5 any device still can enable
  - » Now monitored via Threat History Widget
    - Requires SSHD
    - Requires Non-SOHO device

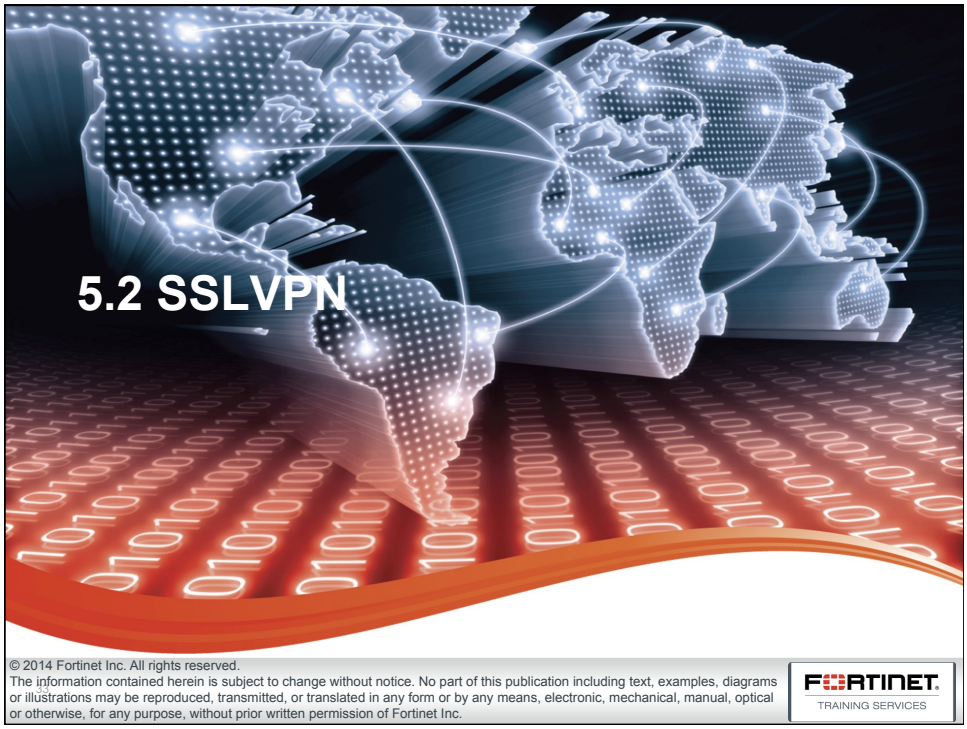
31

Renamed and Moved

- Renamed to “Threat Weight”
  - » due to link with Threat History widget



32



FORTINET TRAINING SERVICES

SSLVPN: New Features & Changes

- Overall Configuration Change

FORTINET

Feature Overview – Motivation

- In relation to the Identity policy changes, the motivation behind these SSLVPN improvements come from an NFR

"Customer feedback on VPN config is not good regarding doubled up policies, hence the recommendation to put the session establishment right back in the respective subsystems. Keep using the policy engine for traffic forwarding policy purposes - SSLVPN and interface-mode IPSEC."

"Elimination of the perceived complexity of the existing engine"

35

Feature Overview – Remove SSL-VPN Policy Sub-type

- tunnel mode and web mode configurations will be unified
- identity-based configuration will be removed
- policy definition will be consistent with firewall policy in 5.2
- Changes:
  - user can create 1 policy that covers both tunnel & web mode (as enabled), and the SSL daemon will take care of installing the necessary policies to the kernel
  - Services will be used to also control the web portal service options (currently found in SSL Portal Profile)
  - action will be allow/deny
  - user/group will be configured, and also used for authentication
  - Select "ssl.root (sslvpn tunnel interface" as source
  - Device identification is not an option

36

Feature Overview – Prompt for conflict of ssl-vpn and admin GUI

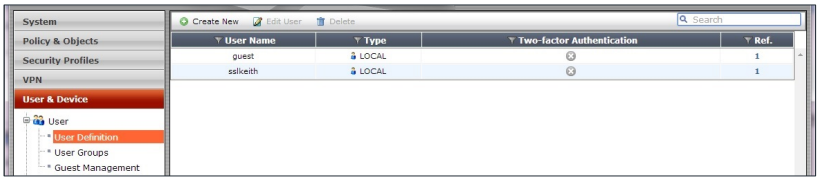
- Our default admin HTTPS GUI port is 443. Also, the default SSL-VPN port is 443.
- When both are enabled on the same interface, it will cause a conflict.
- The default is that when both are enabled, we should let SSL-VPN take a higher priority, this means when user connect to 443 port that has both admin GUI and SSL-VPN, we only show SSL-VPN GUI.
- We should have some a warning prompt in FOS to alert user of this conflict.

Feature Overview – SSL VPN GUI 'Settings' Improvements

- The current VPN > SSL > Settings page presents a big list of random options which are not very easy to understand, especially for low end users:
  - Restricting Source IP is more like optional and not the most important setting
  - "Port Precedence" is very confusing what it's related to
  - Assigning the IP Pool in this place only is useful for multiple portal scenarios that want to use overlapping IP range (rare in low end)
  - The items are not organized in an intuitive way
- New GUI consolidates these settings

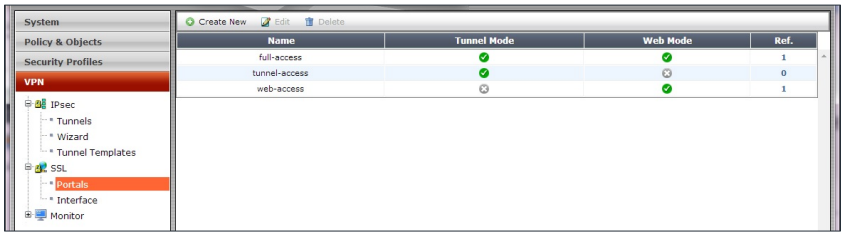
Basic Setup, Step 1 – User/User Groups

1. Define the user/user groups to be allowed by the SSLVPN



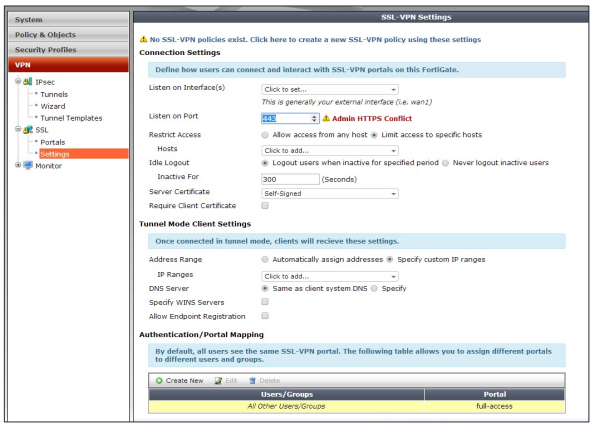
Basic Setup, Step 2 – VPN->SSL->Portals configuration

2. Add/Modify Portals adjust the behaviour of Web and Tunnel mode SSLVPN portals that users are presented with after login



Basic Setup, Step 3 – VPN->SSL->Settings

3. Configure the SSLVPN interface settings under VPN->SSL->Settings



While the port conflict doesn't pose any problems initially, it will take over your admin session if this is not changed after the rest of the config is defined

Basic Setup, Step 3 – Limiting Access

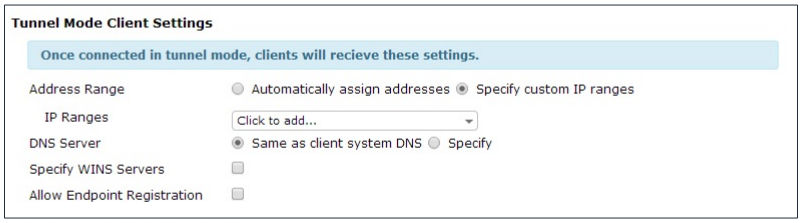
- "Listen on Interface(s)" allows user to specify which interface(s) to accept client connections from. This replaces the need to configure a *wan->internal* policy for portal access in 5.0
- Further restrictions can be applied with the "Restrict Access" Hosts list

Basic Setup, Step 3 – Negated addresses

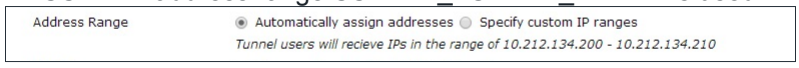
- a source-address-negate option in CLI enables users to apply negation to the list of hosts, thereby setting a list of “Restrict Access” hosts to disallow

```
FGT60C # config vpn ssl settings
FGT60C (settings) # set ?
...
source-interface            SSL VPN source interface of incoming traffic.
source-address              Source address of incoming traffic.
source-address-negate       Enable/disable negated source address match.
source-address6             IPv6 source address of incoming traffic.
source-address6-negate      Enable/disable negated source IPv6 address match.
...
FGT60C (settings) # set source-address-negate enable
FGT60C (settings) # set source-address PC1
```

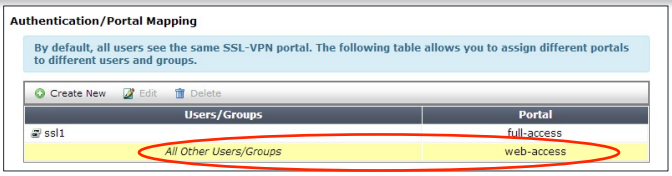

Basic Setup, Step 3 – Tunnel mode



- The Tunnel Mode Settings are defaults that apply to all tunnel mode configs
- The Address Range applies to all tunnels that have not explicitly defined a range under the SSL->Portals Profiles
- If the Automatically assign addresses option is chosen, the default SSLVPN address range SSLVPN_TUNNEL_ADDR1 is used



Basic Setup, Step 3 – Default Portal & portal options



- Instead of configuring user groups & portal mapping under the Identity-based policy (like 5.0), this is done under the SSL-VPN Settings page
- "default-portal" allows users/groups not defined in the mapping to map to a default portal. Proper firewall policies are still required for access
  - Setting a default portal is required

```
FGT60C # config vpn ssl settings
FGT60C (settings) # show
config vpn ssl settings
...
    set default-portal "web-access"
    config authentication-rule
        edit 1
            set groups "ssl1"
            set portal "full-access"
        next
    end
end
```

```
FGT60C (settings) # config authentication-rule
FGT60C (authentication-rule) # edit 1
FGT60C (1) # set
source-interface    SSL VPN source interface of incoming traffic.
users               User name.
groups              User groups.
portal              SSL VPN portal.
realm               SSL VPN realm.
client-cert         Enable/disable SSL VPN client certificate restrictive.
cipher              SSL VPN cipher strength.
auth                SSL VPN authentication method restriction.
```


Basic Setup, Step 3 – Split Tunneling

- The new "Routing Address" option on GUI ensures the addresses in that list are routed through the FortiGate, while Split Tunneling is enabled


```
config vpn ssl web portal
    edit "full-access"
        ....
        set split-tunneling-routing-address "192.168.77.0-Subnet"
        ....
    next
end
```

- Upon connection from a PC, routes to this subnet are directed to the SSLVPN GW

```
C:\Users\keithli>route print 192.168.77.0

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
     192.168.77.0    255.255.255.0   10.212.134.201   10.212.134.200     20
===========================================================================
```

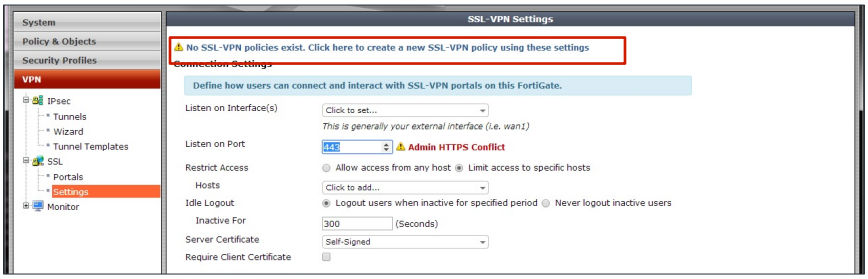
Basic Setup, Step 4 – Firewall Policy configurations

4. Create the appropriate firewall policies to authenticate users and allow tunnel mode access
   - » In 5.0, a *wan->internal* sslvpn identity based policy with an action of SSLVPN was needed to allow both web and tunnel mode traffic to authenticate and pass through
   - » Respective *ssl.root->internal* policies were created automatically per "auto-tunnel-policy enable" option
   - » In 5.2, the *ssl.root->internal* policy with an action of accept is needed for successful authentication and allowing traffic to pass through into the Lan
   - » *ssl.root->WAN* requires if traffic will enter an SSLVPN tunnel from the LAN

47

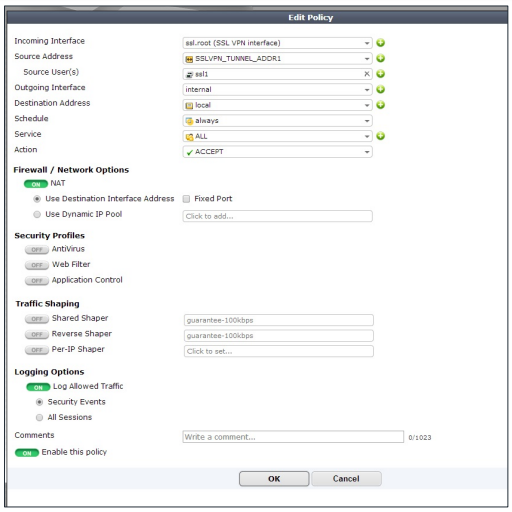
Basic Setup, Step 4 – Firewall Policy configurations

- Before a ssl.root->internal firewall policy is created, users can neither access web mode nor tunnel mode
- Message on the VPN->SSL->Settings page warns of this



48

Basic Setup, Step 4 – Firewall Policy configurations



To allow both web mode and tunnel mode access, only 1 firewall policy is required

Incoming Interface: ssl.<*vdom*>

Source Address: *specify the address range provided for tunnel mode access. This field is meaningless for web mode*

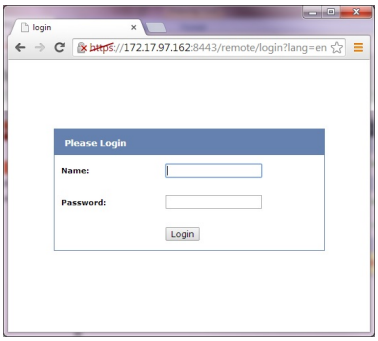
Source User(s): *specify the user group(s) defined in the auth/ profile mapping under the VPN->SSL->Settings page*

Outgoing Interface: *specify the network to allow access for*

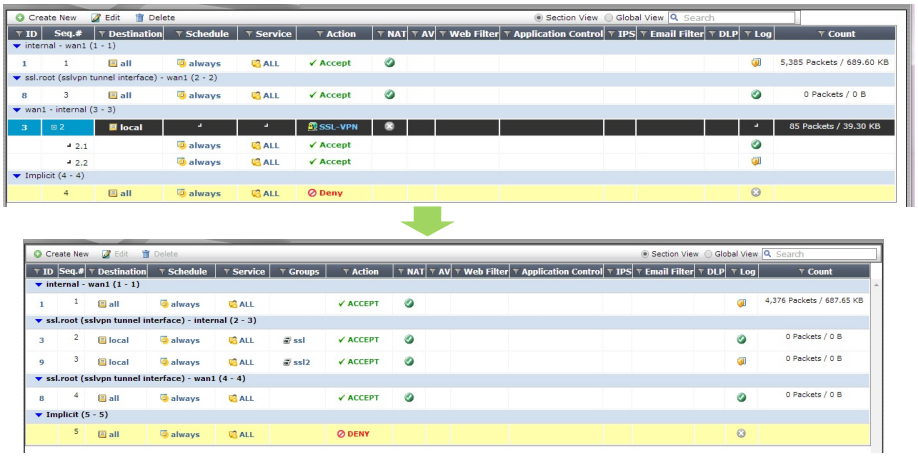
Destination Address: *specify only the network that is being allowed*

Basic Setup, Step 4 – Firewall Policy configurations

- Once the policy is created, you will notice 2 things:
  - This opens up access to the web portal
  - The Source access is defined by the “Restrict Access” hosts list



Upgrade – A Basic scenario



» Note the changes to firewall policies

Upgrade

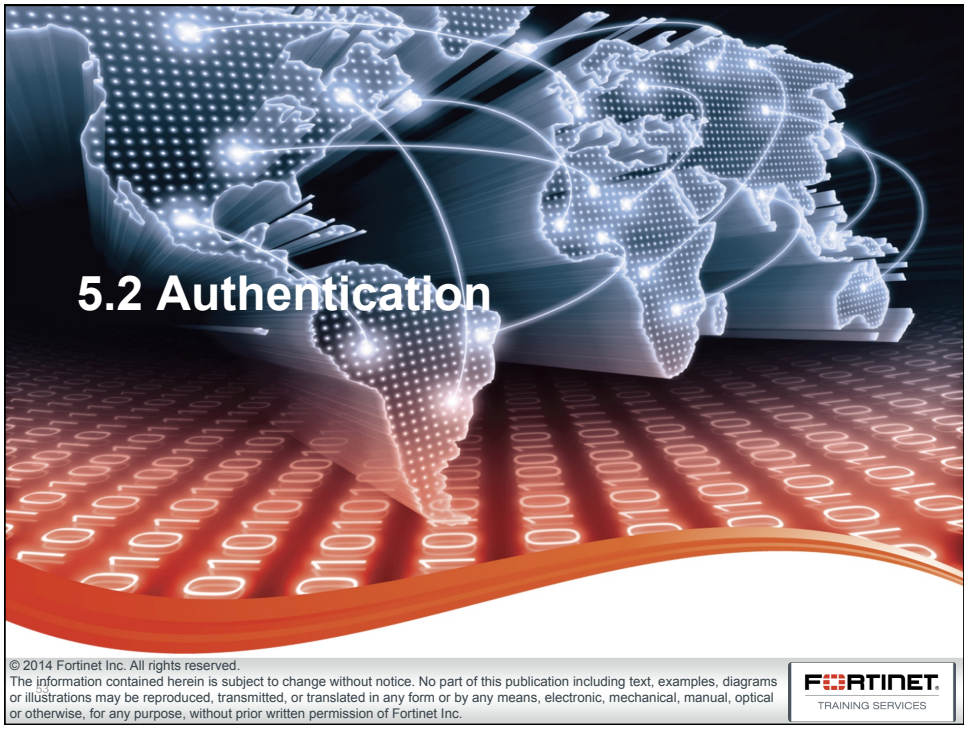
» The wan->internal policy has been replaced by a listening interface

» ssl.root->internal policies replace the ID based policies

» sslvpn-portal option is moved to SSL->Settings

```
config firewall policy
edit 3
    set srcintf "wan1"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "local"
    set action ssl-vpn
    set identity-based enable
        config identity-based-policy
            edit 1
                set schedule "always"
                set logtraffic all
                set groups "ssl"
                set service "ALL"
                set sslvpn-portal "full-access"
            next
            edit 2
                set schedule "always"
                set groups "ssl2"
                set service "ALL"
                set sslvpn-portal "web-access"
            next
        end
    next
```

```
config firewall policy
edit 3
    set srcintf "ssl.root"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "local"
    set action accept
    set schedule "always"
    set service "ALL"
    set logtraffic all
    set groups "ssl"
    set nat enable
next
edit 9
    set srcintf "ssl.root"
    set dstintf "internal"
    set srcaddr "all"
    set dstaddr "local"
    set action accept
    set schedule "always"
    set service "ALL"
    set groups "ssl2"
    set nat enable
next
```



FORTINET TRAINING SERVICES

Authentication: New Features

- New Authentication server type
- Maximum number of Guest users
- SSO_guest_user behavior

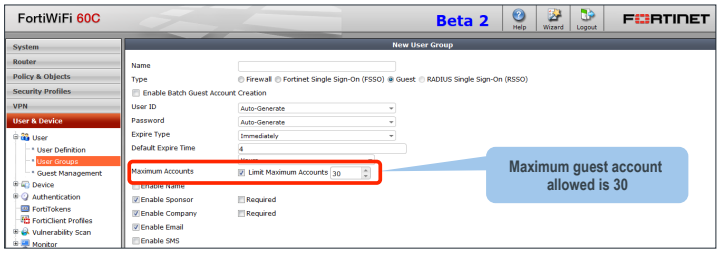
FORTINET

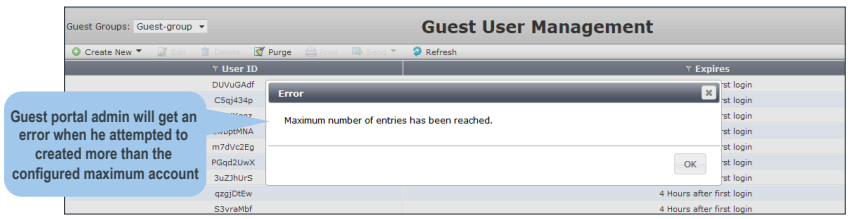
New Authentication server type: POP3/POP3S

- Authentication can now be done through an external POP3/POP3S server
  - » Users would authentication using their email address and email password

Maximum number of Guest users

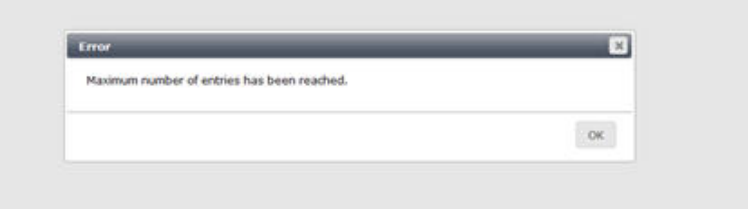
- Limit the maximum number of **guest user** per **guest user portal**





Maximum number of Guest users: Administration

- If an administrator or Guest User Administrator attempts to create more guest accounts then maximum allowed for that group, they will get an error message.



57

SSO_guest_user group behavior

- If only passive authentication is enabled, and the user is not part of any other group, then they will be considered part of SSO_guest_user
- If passive and active authentication is used and the user cannot be determined passively, then active authentication will determine the user.
  - » Group membership will be based on the active username

58

FORTINET TRAINING SERVICES

SNMP: New Features & Changes

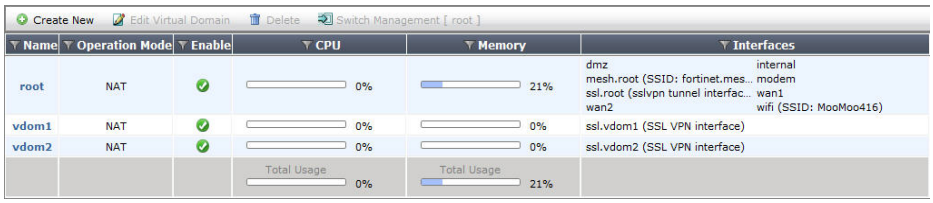
- USB Modem
- Per VDOM CPU & Memory
- AES256 support

FORTINET

USB Modem: Logs & Traps on detection and removal

- SNMP Traps and Log messages will be create when a USB modem is plugged in as well as when it is removed
  - » Details include vendor id and product id for proper device identification

Per VDOM CPU 7 Memory levels: Estimated



LabLocation_Charlie (global) # diag sys vd stats
vdom2 cpu:0% mem:0%
vdom1 cpu:0% mem:0%
root cpu:0% mem:21%

AES256 Support

- Can be enabled from the CLI

```
config system snmp user
        edit "test"
        set priv-proto aes256
        next
end
```

- No GUI support to set AES256 at this time
  - » At the moment most SNMP software does not have the option to use AES256
  - » Setting is available if there is a security policy in place that requires it

63

End

64